**Deutscher Bundestag** **Drucksache 19/25561**

**19. Wahlperiode** 22.12.2020

# Kleine Anfrage

**der Abgeordneten Dr. Wieland Schinnenburg, Stephan Thomae, Renata Alt, Christine Aschenberg-Dugnus, Nicole Bauer, Jens Beeck, Dr. Jens Brandenburg (Rhein-Neckar), Sandra Bubendorfer-Licht, Dr. Marco Buschmann, Christian Dürr, Dr. Marcus Faber, Daniel Föst, Otto Fricke, Reginald Hanke, Peter Heidt, Katrin Helling-Plahr, Markus Herbrand, Torsten Herbst, Dr. Gero Hocker, Manuel Höferlin, Reinhard Houben, Ulla Ihnen, Olaf in der Beek, Pascal Kober, Carina Konrad, Konstantin Kuhle, Ulrich Lechte, Alexander Müller, Dr. Martin Neumann, Matthias Seestern-Pauly, Dr. Hermann Otto Solms, Bettina Stark-Watzinger, Benjamin Strasser, Katja Suding, Manfred Todtenhausen, Nicole Westig, Katharina Willkomm und der Fraktion der FDP**

## Datensicherheit des besonderen elektronischen Anwaltspostfachs

Die Bundesrechtanwaltskammer (BRAK) hat am 28. November 2016 für jeden Rechtsanwalt in Deutschland ein besonderes elektronisches Anwaltspostfach (beA) eingerichtet (erreichbar über www.bea-brak.de). Nach anfänglichen Startproblemen und gerichtlichen Auseinandersetzungen ist das beA für alle Rechtsanwälte seit 1. Januar 2018 zu nutzen (https://www.lto.de/recht/juristen/b/brak-praesident-bea-anwaelte-rechtsstaat-datenschutz). Auch von Unstimmigkeiten bei der Begutachtung von Sicherheitsrisiken war die Rede (https://www.golem.de/news/bundesrechtsanwaltskammer-originalfassung-von-bea-sicherheitsgutachten-freigeklagt-2010-151190.html). Die Anforderungen an das Sicherheitslevel des beA scheinen mittlerweile geklärt zu sein (https://www.heise.de/newsticker/meldung/Gericht-Durchgehende-Verschluesselung-beim-Anwaltspostfach-nicht-noetig-4586672.html), allerdings wirft der Wechsel vom bisherigen Dienstleister Atos zu Wesroc neue Sicherheitsfragen auf. Es sei nicht auszuschließen, dass der alte Dienstleister noch über Sicherheitsschlüssel verfüge. Darauf hatte ein Sachverständiger in der Sitzung des Rechtsausschusses am 16. November 2020 hingewiesen. Es bestehe die Gefahr, dass die gesamte Kommunikation, die über das beA abgewickelt wird, mitgelesen werden könne. Über eine Ende-zu-Ende-Verschlüsselung, die das verhindern würde, verfüge das beA nicht. Aus Sicht eines Experten sollte deshalb zügig auf die Herstellung neuer Sicherheitsschlüssel hingewirkt werden. Die Frage, ob der rechtmäßige Betrieb des beA eine Ende-zu-Ende-Verschlüsselung erfordert, liegt dem Bundesgerichtshof zur Beantwortung vor (AnwZ (Brfg) 2/20). Durch Unsicherheiten in der Nutzung der elektronischen Infrastruktur leidet das Vertrauen der Bürger in den elektronischen Rechtsverkehr. Das muss nach Ansicht der Fragesteller verhindert werden.

Wir fragen die Bundesregierung:

1. Trifft es nach Kenntnis der Bundesregierung zu, dass die BRAK beziehungsweise ihre technischen Dienstleister rein technisch jede Nachricht entschlüsseln können?
   a) Wenn ja, wie ist diese Zugriffsmöglichkeit mit dem Schutz der Vertraulichkeit von Anwalt-Mandanten-Korrespondenz zu vereinbaren?
   b) Wenn nein, warum wurde der Hinweis laut eines Pressebericht im Originalgutachten der Secunet Security Networks AG entfernt (https://www.golem.de/print.php?a=151190)?
   c) Liegen die Daten während der Umschlüsselung unverschlüsselt vor und könnten diese Daten von Dritten oder von der BRAK gelesen werden?
2. Wie wird ein „sicherer Übermittlungsweg“ im Sinne des § 130a der Zivilprozessordnung (ZPO) sichergestellt?
3. Wie wird der Verzicht auf eine Ende-zu-Ende-Verschlüsselung beim beA nach Kenntnis der Bundesregierung begründet?
4. Wie wird bzw. ist ausgeschlossen, dass Dritte einen Zugriff auf den „privaten Schlüssel“ erhalten?
   a) Wie wurde sichergestellt, dass durch den Wechsel der Dienstleister keine Kopien der „privaten Schlüssel“ erstellt wurden?
   b) Wären (rein theoretisch) Konstellationen denkbar, in denen es möglich wäre, auf die „privaten Schlüssel“ Zugriff zu erhalten?
   c) Trifft es zu, dass die „privaten Schlüssel“ ohne Aufsicht der BRAK erstellt wurden?
5. Ist aus der Sicht der Bundesregierung erforderlich, dass auf die Herstellung neuer Schlüssel hingewirkt wird?
   a) Wenn ja, welche Schritte unternimmt sie?
   b) Wenn nein, warum nicht?
   c) Wie oft werden die jeweilig verwendeten Schlüssel und Zertifikate jeweils erneuert?
6. Welche Schwachstellen beim beA sind nach Freischaltung aufgedeckt und beseitigt worden (bitte anhand Zeitstrahl detailliert auflisten)?
7. Gibt es aktuell Sicherheitslücken, an deren Behebung nach Kenntnis der Bundesregierung aktuell gearbeitet wird?
   a) Wenn ja, welche sind das, und bis wann werden sie behoben?
   b) Wenn nein, wie werden Sicherheitslücken ausgeschlossen, bzw. woran kann man das Nichtbestehen solcher Lücken festmachen?
8. Wie wird das aktuelle Sicherheitsregelwerk beschrieben?
9. Wie und durch wen werden Störungen der IT-Sicherheitsarchitektur nach Kenntnis der Bundesregierung behoben?
   a) Gibt es einen Notfallplan, und wie sieht er aus?
   b) Wenn nein, warum nicht?
10. Welche Sicherheitstests und Sicherheitsanalysen des beA hat es nach Kenntnis der Bundesregierung bisher gegeben, und was waren jeweils die Ergebnisse?

11. Auf welcher Serverarchitektur wird das beA nach Kenntnis der Bundesregierung betrieben?
    a) Welche Betriebssysteme in welcher Version werden verwendet?
    b) Welche Webserver-Software in welcher Version wird verwendet?
    c) Welche Webserver-Module und Erweiterungen in welchen Versionen werden verwendet?
12. Ist es nach Kenntnis der Bundesregierung geplant, die Authentifizierung beim beA zu vereinfachen und etwa auch eine App-basierte Authentifizierung oder weitere Verfahren einzuführen?
13. Ist nach Kenntnis der Bundesregierung eine Offenlegung des beA-Quellcodes geplant?
    a) Sollten Lizenzrechte Dritter einer vollständigen Offenlegung entgegenstehen, ist eine teilweise Offenlegung der übrigen Teile des Quellcodes geplant?
    b) Falls nein, warum nicht?
14. Hat die Bundesregierung Kenntnis über Pläne die Weiterentwicklung hin zu einem sogenannten beA 2.0 betreffend, welches konzeptionelle Schwächen der aktuellen Version, insbesondere den Verzicht auf durchgehende Ende-zu-Ende-Verschlüsselung, angeht?

Berlin, den 8. Dezember 2020

**Christian Lindner und Fraktion**

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333